Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of the Claims:

1. (Currently Amended) A method ~~for preventing unauthorized access to hardware management information~~ comprising:

receiving a request for hardware component information in a service processor disposed in a hardware component as an open session request from a requesting client application, which request passed to the service processor external to an operating system controlling the hardware component;

transmitting from the service processor a challenge string to the requesting client application, the challenge string includes a sequence number that increments with each new session;

receiving in the service processor a challenge response from the requesting client application, the response including a hash number that is a function of at least one of the challenge string, session identification number, sequence number, and a password;

comparing the challenge response to an expected response to the challenge string; and

transmitting hardware component information to the requesting client application.

2. (Canceled)

3. (Original) The method according to claim 1, wherein the challenge response includes a session identification number unique to each session and assigned by the service processor.

4. (Previously Presented) The method according to claim 1, wherein the challenge response includes a sequence number that increments with an every new message.

5. (Canceled)

6. (Original) The method according to claim 1, further comprising examining each packet received from the client application for one or more of the following: the session identification number, the sequence number and a hash number.

7. (Original) The method according to claim 6, wherein the hash number is a function of one or more of the following: the session identification number, the sequence number and the packet itself.

8. (Currently Amended) A method ~~for preventing unauthorized access to hardware management information~~ comprising:

transmitting a request for hardware component information to a service processor disposed in a hardware component as an open session request from a requesting client application, the request to be passed to the service processor external to an operating system controlling the hardware component;

~~passing the request to the service processor external to an operating system controlling the hardware component~~;

receiving from the service processor a challenge string at the requesting client application, the challenge string includes a sequence number that increments with each new session;

transmitting to the service processor a challenge response from the requesting client application, the response including a hash number that is a function of at least one of the challenge string, session identification number, sequence number, and a password; and

receiving from the service processor an authentication response to the requesting client application based on a comparison of the challenge response from the requesting client application and an expected challenge response calculated in the service processor.

9. (Original) The method according to claim 8, wherein the challenge string includes a session identification number assigned by the service processor, which

session identification number is unique to each session, and the challenge response includes the session identification number.

10. (Canceled)

11. (Canceled)

12. (Original) The method according to claim 8, further comprising transmitting with each packet sent by the client application one or more of the following: the session identification number, the sequence number and a hash number, and the hash number is a function of one or more of the following: the session identification number, the sequence number and the packet itself.

13. (Currently Amended) An apparatus ~~for authenticating a client application requesting access to a particular component among a plurality of components,~~ comprising:

a remote access port; and

a service processor ~~disposed in the particular component,~~ coupled to the remote access port~~;~~ ~~and~~

the service processor including a machine readable medium, having stored thereon a set of instructions, which when executed perform method comprising of:

in response to a remote request for information about ~~the particular~~a component received as an open session request through the remote access port external to a host operating system of the apparatus, the service processor ~~is programmed to:~~

~~———~~transmiting a challenge string to a requesting client application, the challenge string includes a sequence number that increments with each new session;

comparinge a challenge response received from the requesting client application with an expected response to the challenge, the response including a hash number that is a function of at least one of the challenge string, session identification number, sequence number, and a password; and

transmitting an authentication response to the requesting client application based on the comparison.

14. (Canceled)

15. (Original) The apparatus according to claim 14, wherein the service processor reviews the challenge response to determine if it contains the session identification number transmitted in the challenge string.

16. (Original) The apparatus according to claim 13, wherein the service processor compares a sequence number included in the challenge response against previously received sequence numbers and ignores the challenge response if it does not include a sequence number in correct sequence.

17. (Original) The apparatus according to claim 13, wherein the service processor compares a hash number received in the challenge response with an expected hash calculated by the service processor and transmits a success or failure message depending upon a result of the comparison.

18. (Canceled)

19. (Canceled)

20. (Currently Amended) A system ~~for accessing hardware component information from a computer,~~ comprising:

~~a service processor disposed in the computer;~~

~~a server being coupled to each of the service processors in the computer;~~

a processor;

a memory; and

a client application stored on a machine readable medium, the client application including a set of instructions which when executed, perform a

method of:~~to execute on the server, wherein the service processor authenticates requests from the client application requesting access to the service processor's host hardware module, which request bypasses the operating system of the computer, each of said service processor in response to a request for access to the host hardware module is programmed to:~~

transmitting a request for hardware component information to a service processor disposed in a hardware component as an open session request, the request to be passed to the service processor external to an operating system controlling the hardware component;

receiving from the service processor a challenge string at the requesting client application, the challenge string includes a sequence number that increments with each new session;

transmitting to the service processor a challenge response from the requesting client application, the response including a hash number that is a function of at least one of the challenge string, session identification number, sequence number, and a password; and

receiving from the service processor an authentication response to the requesting client application based on a comparison of the challenge response from the requesting client application and an expected challenge response calculated in the service processor.~~transmit a challenge string to a requesting client application;~~

~~compare a challenge response received from the requesting client application with an expected response to the challenge; and~~

~~transmit an authentication response to the requesting client application based on the comparison.~~

21-30 (Canceled)

31. (Currently Amended) ~~An apparatus for preventing unauthorized access to hardware management information comprising a computer readable media having programming instructions encoded thereon, instructing a processor to:~~

A machine readable medium having stored thereon a set of instructions which when executed, perform a method of:

transmitting a request for hardware component information to a service processor disposed in a hardware component as an open session request, the request to be passed to the service processor external to an operating system controlling the hardware component;

receiving from the service processor a challenge string at the requesting client application, the challenge string includes a sequence number that increments with each new session;

transmitting to the service processor a challenge response from the requesting client application, the response including a hash number that is a

function of at least one of the challenge string, session identification number, sequence number, and a password; and

receiving from the service processor an authentication response to the requesting client application based on a comparison of the challenge response from the requesting client application and an expected challenge response calculated in the service processor.~~receive a request for hardware component information in a service processor disposed in a hardware component as an open session request, which request passes external to an operating system controlling the hardware component;~~

~~transmit from the service processor a challenge string to the requesting client application;~~

~~receive in the service processor a challenge response from the requesting client application;~~

~~compare the challenge response to an expected response to the challenge; and~~

~~transmit from the service processor an authentication response to the requesting client application based on the comparison.~~

32. (Currently Amended) A machine readable medium having stored thereon a set of instructions which when executed, perform a method of:~~An apparatus for preventing unauthorized access to hardware management information~~

~~comprising a computer readable media having programming instruction encoded thereon instructing a processor to:~~

transmiting a challenge string to a requesting client application, the challenge string includes a sequence number that increments with each new session;

comparing a challenge response received from the requesting client application with an expected response to the challenge, the response including a hash number that is a function of at least one of the challenge string, session identification number, sequence number, and a password; and

transmitting an authentication response to the requesting client application based on the comparison.~~transmit a request for hardware component information to a service processor disposed in a hardware component as an open session request from a requesting client application, which request passes external to an operating system controlling the hardware component;~~

~~receive from the service processor a challenge string at the requesting client application;~~

~~transmit to the service processor a challenge response from the requesting client application; and~~

~~receive from the service processor an authentication response to the requesting client application based on a comparison of the challenge response~~

~~from the requesting client application and an expected challenge response calculated in the service processor.~~

33. (Canceled)